Managing Active Directory

Daniel Bell
Systems Integration Consultant
Melillo Consulting, Inc
545 Fifth Avenue, Suite 600
New York, NY 10017
Phone: (212) 692-5230
Fax: (212) 692-5239
danb@mjm.com

Contents

- Designing a Management Infrastructure
- Designing NTDS for Effective Management
- Identifying Single Points of Failure
- Tips for Achieving Root Cause Management
- Extending Event Logs and Performance Counters
- Replication Management
- Using Scripting and ADSI

Why Do We Need Management??

- Active Directory is solid, but every Goliath has its David
- Windows 2000 is a distributed, complex environment
- Delegation of Administration can affect IT continuity

Top 10 reasons NTDS fails

- Staff is not trained
- Lack of support staff
- Improper backups
- Network failure
- No proactive monitoring
- Too many compromises made
- Not enough DC’s
- Too Many DC’s
- Poor Active Directory design
- Admin quits to work for IPO firm

Important!!

Train Your Staff

Pedestal Lecture

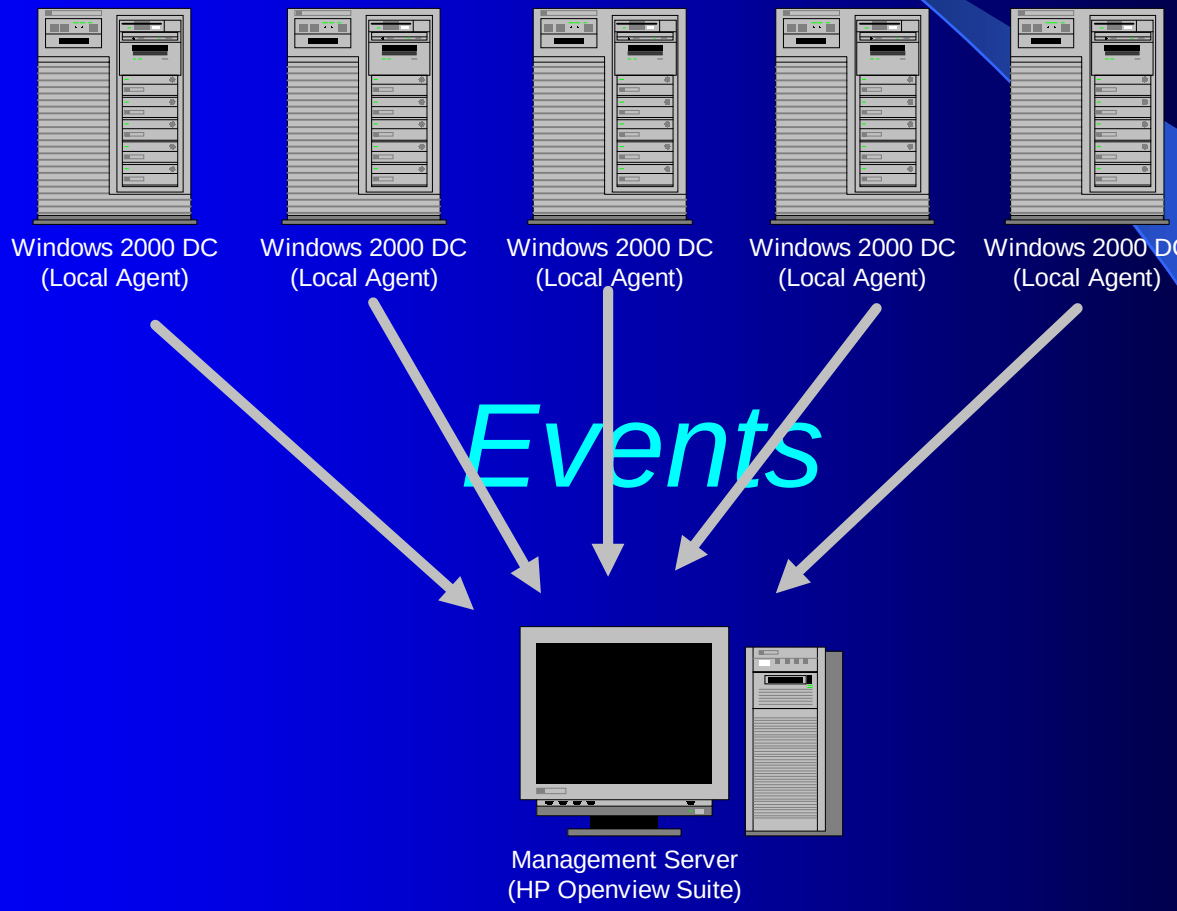
- This is not a PC environment anymore
- An NT 4.0 admin is not an Windows 2000 admin
- Focus on backups
- Maximize availability
- Do not make compromises!

Management Design: Best Practices

- Monitor locally, manage globally
- Management infrastructure design
- Write Once, Manage Everything
- Notification

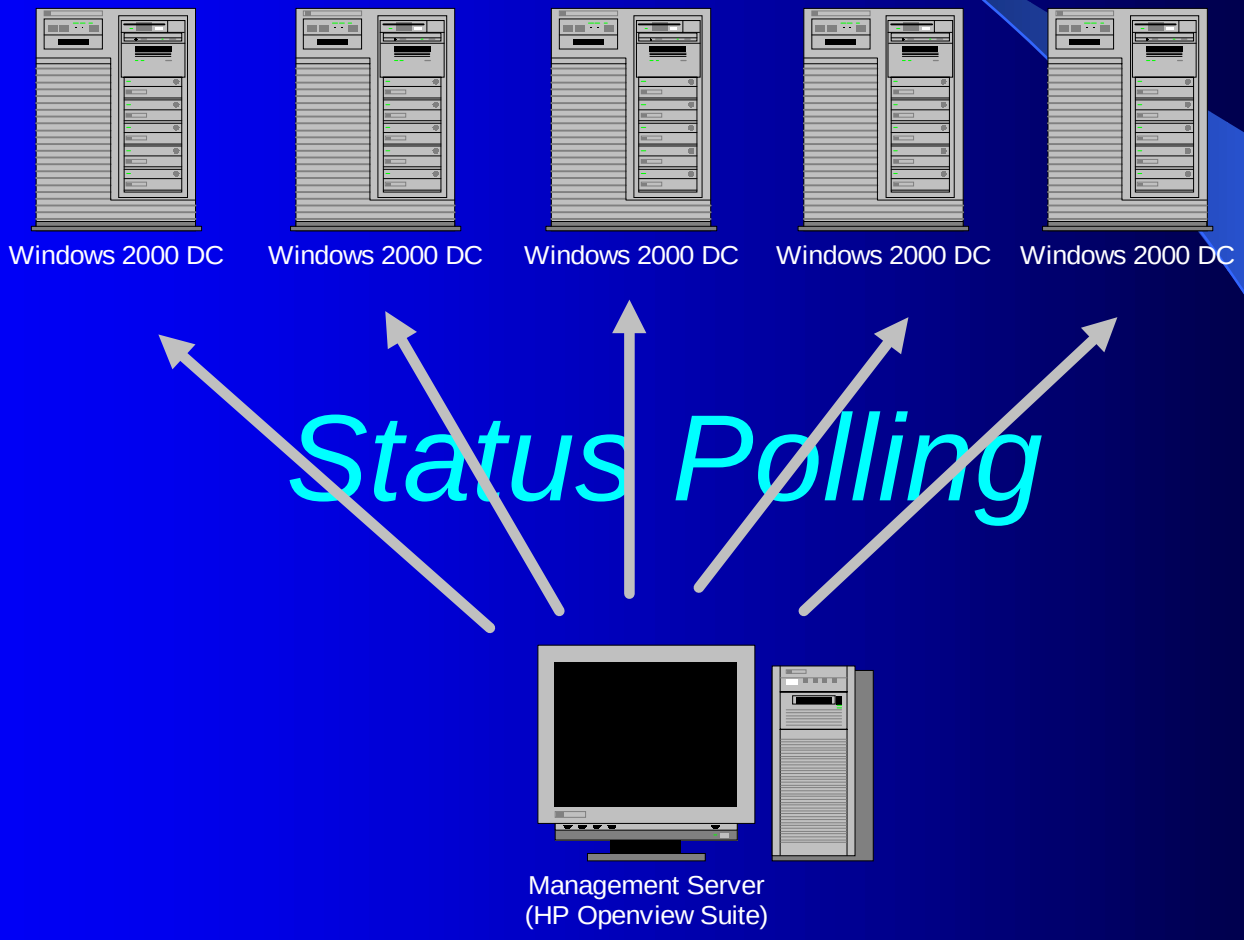
Monitor Locally, Manage Globally

- Top-Down Management (ManageX, Vantage Point for Windows)



Monitor Locally, Manage Globally (2)

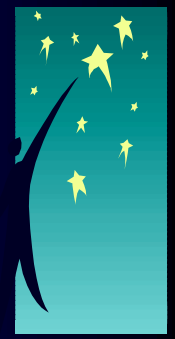
- Bottom-Up Management (Network Node Manager)



Monitor Locally, Manage Globally (3)

- The best management solution is a combination of Top-Down and Bottom-Up management
- An integrated set of products may be needed to achieve this

Management Infrastructure Design



- The Management system should mirror the administrative model of the IT infrastructure
- Large organizations should concentrate on distributing management responsibilities
- With Active Directory Admins, Domain Admins should have a domain view while Container Admins should have a container view

Write Once, Manage Everything

- Monitoring polices may apply to groups of systems
- Group DC’s into monitoring groups
- Apply monitoring polices to groups of systems instead of individual systems

Notification

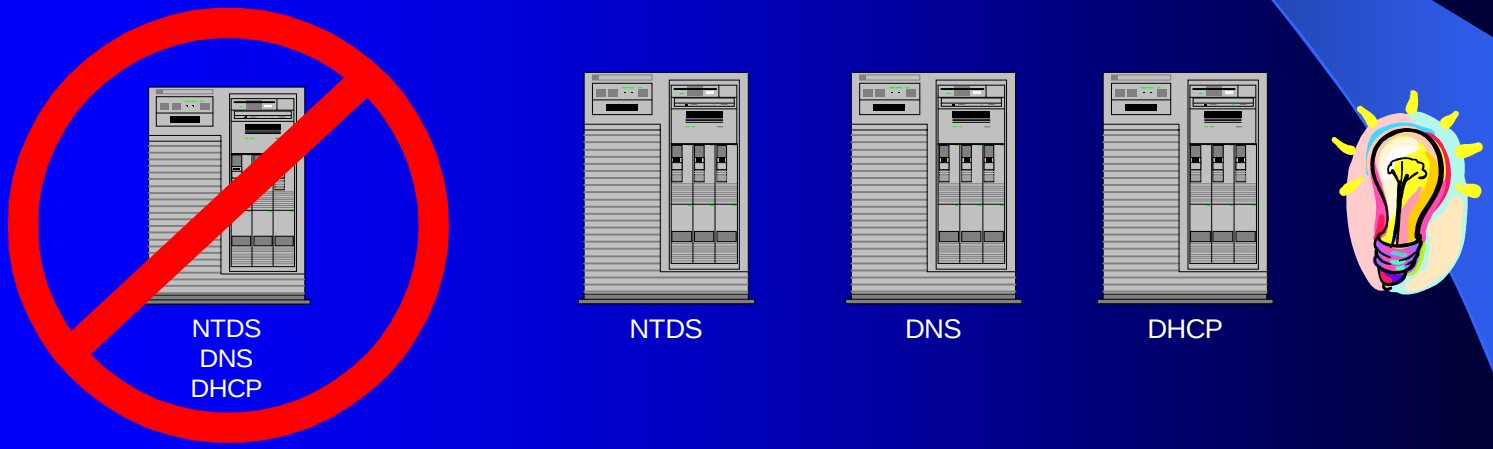
- Just because the operators go home does not mean the Active Directory stops
- Critical events should always be addressed
- A 24/7 operations staff is always a good move
- Paging is a low-cost notification solution

Designing Active Directory

- Dedicated Server Functions
- Strategic Service and Site Placement
- Bridgeheads

Dedicated Server Functions

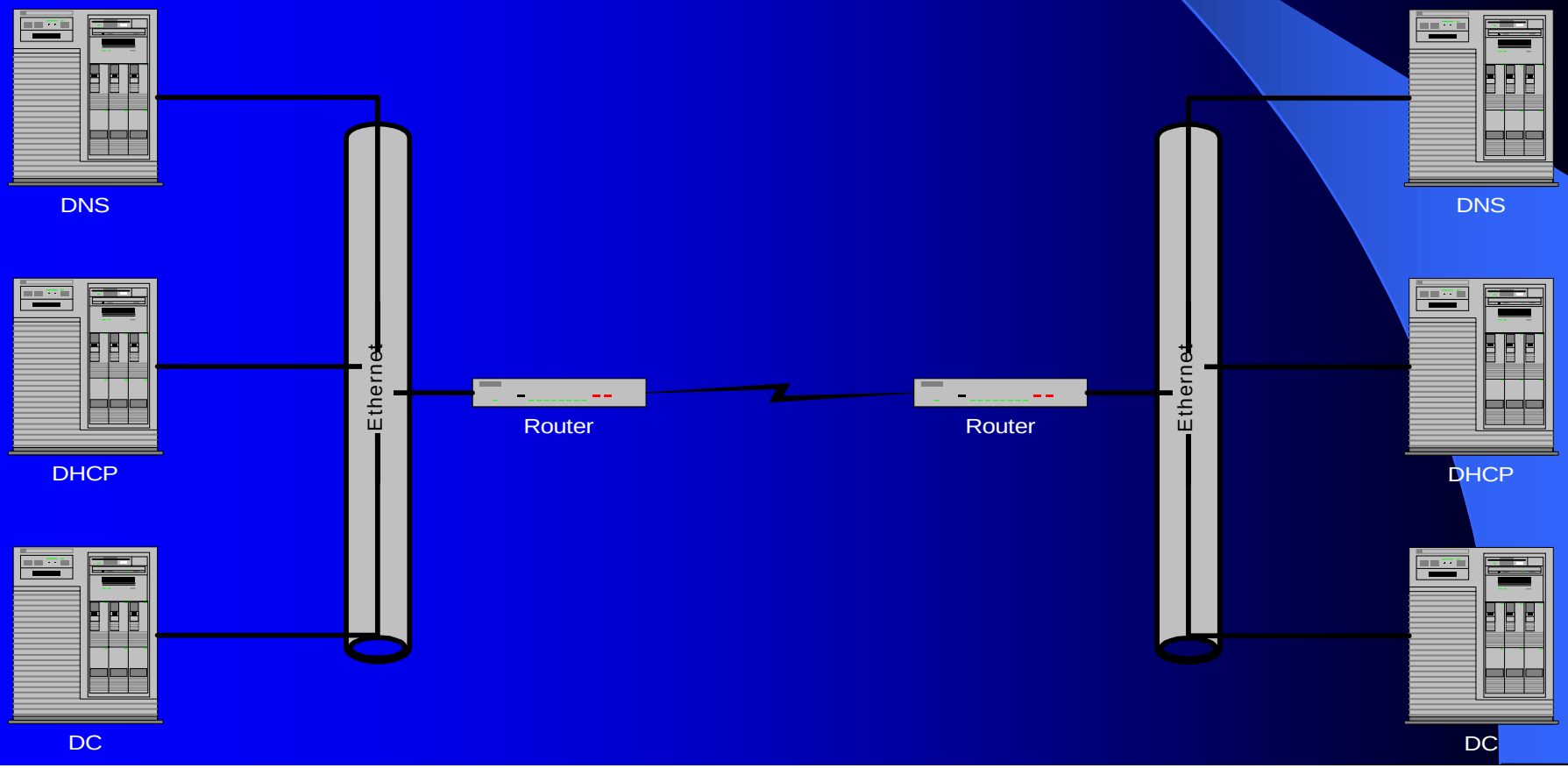
- Each Server should have a dedicated function



- Server failure will only affect one service, not multiples

Service Placement

- Keep WAN failures from immediately affecting AD services
- Services should not span WAN's



Bridgeheads

- Bridgeheads replicate AD between sites
- Site links need to be configured manually
- By default, any DC can act as a Bridgehead
- Windows KCC will automatically configure bridgeheads.
- KCC will usually select DC’s that are closest to the WAN link to act as as Bridgeheads.
- Use Active Directory Replication Monitor to View Selected Bridgeheads

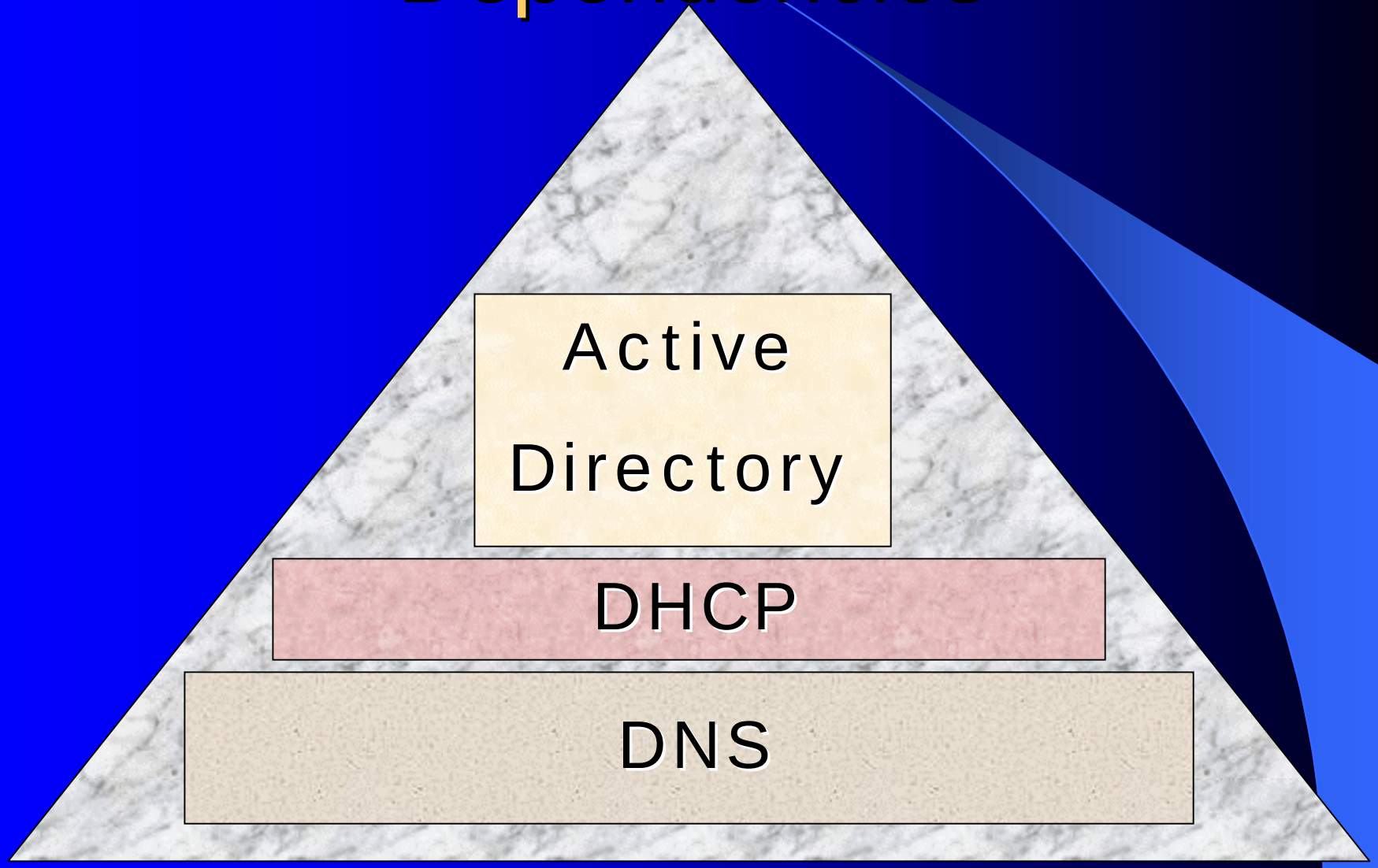
Bridgeheads (2)

- Bridgeheads should run on enterprise hardware
- Bridgeheads *can* be manually selected (see Q244368)
- Keep Bridgeheads close to WAN links
- Monitor bridgeheads robustly

Identifying Single Points of Failure

- DNS
- DHCP

Active Directory Dependencies



DNS

- Active Directory needs DNS to function properly
- Without DNS, DC's are Boat Anchors
- DNS servers must be redundant
- Each Site should have it's own set of DNS servers
- To maximize WAN efficiency, redundant DNS servers should reside on each site
- Use Windows 2000 Active DNS!

DHCP

- DHCP clients are entered into DNS via Windows 2000 DHCP services
- Clients use DNS to locate the closest Login DC
- DCHP service outages can prevent clients and servers from logging into Active Directory
- DHCP should be implemented with redundancy
- Each site should contain redundant DHCP servers

Extending Event Logs and Performance Counters

- Top-Down Management Revisited
- Central Event Monitoring
- Diagnostic Logging
- Policy-Based Performance Monitoring

Top-Down Management Revisited

- Servers manage locally via agents. But report to a management console upon exception
- Operator views and notification reside on the management console

Central Event Monitoring

- The Management Agents should be able to intercept events getting written to the System,Application, and Security Logs
- Manage only by exception, do not confuse operators with useless informational events
- Analyze systems and determine which events should generate alerts
- NTDS Replication Events and Audit Events should be watched carefully
- If necessary, enable diagnostic logging

Enabling Diagnostic Logging

To enable diagnostic event logging,use Registry Editor to change the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics

Valid parameters are:

- 0=None (default)
- 1=Minimum
- 3=Medium
- 5=Maximum

Policy Based Performance Monitoring

- Many Performance Counters ship with Active Directory that allow for proactive performance management
- The Performance Snap-In can measure Performance Counters against thresholds and send alerts if values exceed thresholds
- Do not use The Performance Snap-In!

Policy Based Performance Management (2)

- Local Management Agent technology is a more efficient way to measure performance
- Performance Counter values can monitor locally and events can be sent by exception
- Agent Technology can locally take actions on exception events

Important Active Directory Performance Counters

NTDS.DRA Inbound Bytes Total/Sec

NTDS.DRA Inbound Properties/Sec

NTDS.DRA Outbound Bytes Total/Sec

NTDS.DRA Outbound Properties/Sec

Processor.%Processor Time

Process.% Processor Time

System.%Processor Queue Length

Logical Disk.% Free Space

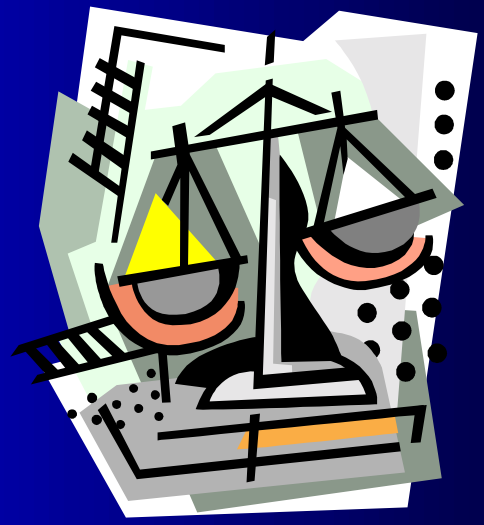
- Diskperf -YV

Tips for Achieving Root Cause Management

- Understand your TCP/IP infrastructure
- Know your Active Directory replication topology (replmon)
- Understand Active Directory dependencies
- Be able to differentiate between inter-site and intra-site replication events
- Know how failures effect your infrastructure
- Use your knowledge to implement Event Correlation Circuits (ECS) that identify the source of the problem

Replication Management

- Know your environment
- NTDS Replication Events and Performance Counters
- Solve issues quickly
- Using DCDIAG



Know Your Environment

- Know your Replication Topology!
- Know the consequences of a replication failure
- Know how to tell inter-site failures from intra-site failures
- Check the network, do not assume an Active Directory problem

NTDS Replication Events and Performance Counters

- Configure Event Management to send events on NTDS replication failures
- Use Performance Counters to gauge NTDS performance
- Use Performance Counters to size how many DC’s are needed
- Too many DC’s can hurt replication performance

Solve Issues Quickly

- Keep an open support contract with Microsoft, this will speed up problem resolution
- Do not make the server available for logins until the problem is solved

Using DCDIAG

- Use DCDIAG to troubleshoot replications

```
DCDIAG /test:Replications
   Testing server: DOMAIN\SERVER1
   Starting test: Replications
   * Replications Check
   [Replications Check,SERVER1] A recent replication attempt failed:
   From SERVER2 to SERVER1
   Naming Context: CN=Schema,CN=Configuration,DC=domain,DC=com
   The replication generated an error (5):
   Access is denied.
   The failure occurred at 1999-12-23 19:54.37.
   The last success occurred at 1999-12-23 15:31.59.
   7 failures have occurred since the last success.
```

- Use your Local Management Agent to retrieve this data at a polling interval

Using Scripting and ADSI

- ADSI is great tool for scheduled maintenance and actions to exception events
- Many administrative tasks can be achieved through ADSI
- Many Management Systems utilize VBScript to collect system information (Performance Counters and Event Log Data)
- VB Script can not only access Performance Counter values, it can also utilize ADSI
- A combination of ADSI and Performance Counters can give operators detailed information

Summary

- A well trained staff is the best way to manage Active Directory
- A Network and Systems management solution is almost a necessity when it come to managing Active Directory
- Replication is the heartbeat of Active Directory, and it should be understood and managed robustly
- ADSI is some really cool stuff. Check it out!

Questions??

Thank You!

Daniel Bell
Melillo Consulting Inc.
545 Fifth Avenue, Suite 600
New York, NY 10017
(212) 692-5230
danb@mjm.com